NCCIC | National Cybersecurity and Communications Integration Center

NCCIC 101

Jeremiah Glenn
Branch Chief
Integrated Threat Analysis Branch

NCCIC

A - 20170802

Overview

The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical infrastructure and communications networks.

NCCIC executes this mission by serving as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating a 24x7 situational awareness, analysis, and incident response center.

> “The cybersecurity functions of the [NCCIC] shall include... being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings... providing shared situational awareness... providing timely incident response capabilities to Federal and non-Federal entities...”
>
> - NATIONAL CYBERSECURITY PROTECTION ACT OF 2014

Authorities

- 🟦 Presidential Directive
- 🟩 Executive Order
- ⬛ Legislative
- 🟦 DHS
- 🟧 NCCIC

2009 OCTOBER

Secretary Janet Napolitano establishes the NCCIC on October 30 with a ribbon cutting ceremony at the culmination of National Cybersecurity Awareness Month.

2010

The NCCIC develops an initial strategy and Concept of Operations, defining its mission and integrating operational and watch floor elements of ICS-CERT, NCC, and US-CERT.

2010

The NCCIC incorporates the National Cyber Exercise and Planning Program and leads Cyber Storm III.

2011 OCTOBER

Presidential Policy Directive-8 (PPD-8), National Preparedness, requires systematic preparation for the threats that pose the greatest risk, including terrorism and cyber attacks.

2012

The NCCIC fully incorporates ICS-CERT, NCC, US-CERT, and NCCIC Operations and Integration into the overarching integrated organization.

2012

Executive Order (EO) 13618, Assignment of National Security and Emergency Preparedness Communications Functions, disbands the National Communications System; NCC consequently assumes significant NS/EP communications responsibilities.

2013

The NCCIC adds the National Cybersecurity Assessment and Technical Services (NCATS) team, providing state-of-the-art cyber assessment and penetration testing services.

2013 FEBRUARY

EO 13636, Improving Critical Infrastructure Cybersecurity, provides guidance to build public-private partnerships, information sharing capabilities, and standards to maintain a healthy cyber-environment.

2013 FEBRUARY

PPD-21, Critical Infrastructure Security and Resilience, identifies and requires the integration of two DHS-operated national critical infrastructure centers—one for physical infrastructure [NICC] and another for cyber infrastructure [NCCIC].

2013 DECEMBER

The **National Infrastructure Protection Plan** describes the NICC/NCCIC integration, risk management framework, and public-private partnerships required to secure the Nation's physical and cyber infrastructure.

Authorities – CONTINUED

🟦 Presidential Directive
🟩 Executive Order
⬛ Legislative
🟦 DHS
🟧 NCCIC

2014

DHS's **Quadrennial Homeland Security Review** and **2014-2018 Strategic Plan** identify the NCCIC as the DHS cyber and communications security operations hub and identify core information sharing, watch, and incident response capabilities.

2014 DECEMBER

The **National Cybersecurity Protection Act of 2014** establishes the NCCIC in law and recognizes its critical role in cyber information sharing, provision of technical assistance, and cyber incident response to the private sector.

2014 DECEMBER

The **Federal Information Security Modernization Act of 2014** authorizes DHS to provide operational and technical assistance to Federal Government civilian agencies and establishes a federal information security incident center within DHS, a function fulfilled by the NCCIC/US-CERT.

2015 FEBRUARY

EO 13691, Promoting Private Sector Cybersecurity Information Sharing, requires the NCCIC to engage Information Sharing and Analysis Organizations in continuous and inclusive sharing of cybersecurity information and address risks and incidents.

2015 DECEMBER

The Cybersecurity Act of 2015 designates the NCCIC as the central hub for the sharing of cyber threat indicators between the private sector and the Federal Government.

2016 FEBRUARY

The **Cybersecurity National Action Plan** calls for DHS—through the NCCIC—to increase its Federal civilian cyber defense teams to a total of 48.

2016 JUNE

The **National Response Framework** (Third Edition) reaffirms CS&C's lead role—performed by the NCCIC/NCC and the Office of Emergency Communications—in coordinating public and private efforts to restore communications infrastructure following an incident.

2016 JULY

PPD-41, United States Cyber Incident Coordination, establishes the NCCIC as the lead coordinator for asset response during a significant cybersecurity incident.

2016 JULY

The NCCIC incorporates the Cyber Information Sharing and Collaboration Program (CISCP); CISCP includes more than 160 private sector participants.

Core Functions

NCCIC performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:

- Information sharing
- Operational planning, training, and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Watch floor operations
- Hunt, incident response, and recovery

FAST FACTS

DHS created NCCIC to lead federal efforts that address threats and incidents affecting the nation's critical infrastructure and communications networks.

NCCIC

NCCIC is a part of the Office of Cybersecurity and Communications (CS&C) within DHS' National Protection and Programs Directorate.

24×7

NCCIC Personnel operate across three physical locations in Arlington, VA; Pensacola, FL; and Idaho Falls, ID. All three locations contribute to the NCCIC's 24x7 watch operations.

Arlington and Idaho Falls house two laboratories: the Advanced Malware Analysis Center, and a control systems-focused Advanced Analytic Laboratory, respectively.

Priorities

Increase national situational awareness of cyber and communications security through a common operational picture and automated, real-time sharing of threat information.

24/7 DAILY

Reduce the duration and severity of cyber and communications incidents by providing comprehensive incident response and recovery services.

Help customers manage cyber and communications threats and vulnerabilities by providing timely and accurate analysis, mitigation recommendations, and steady-state best practices.

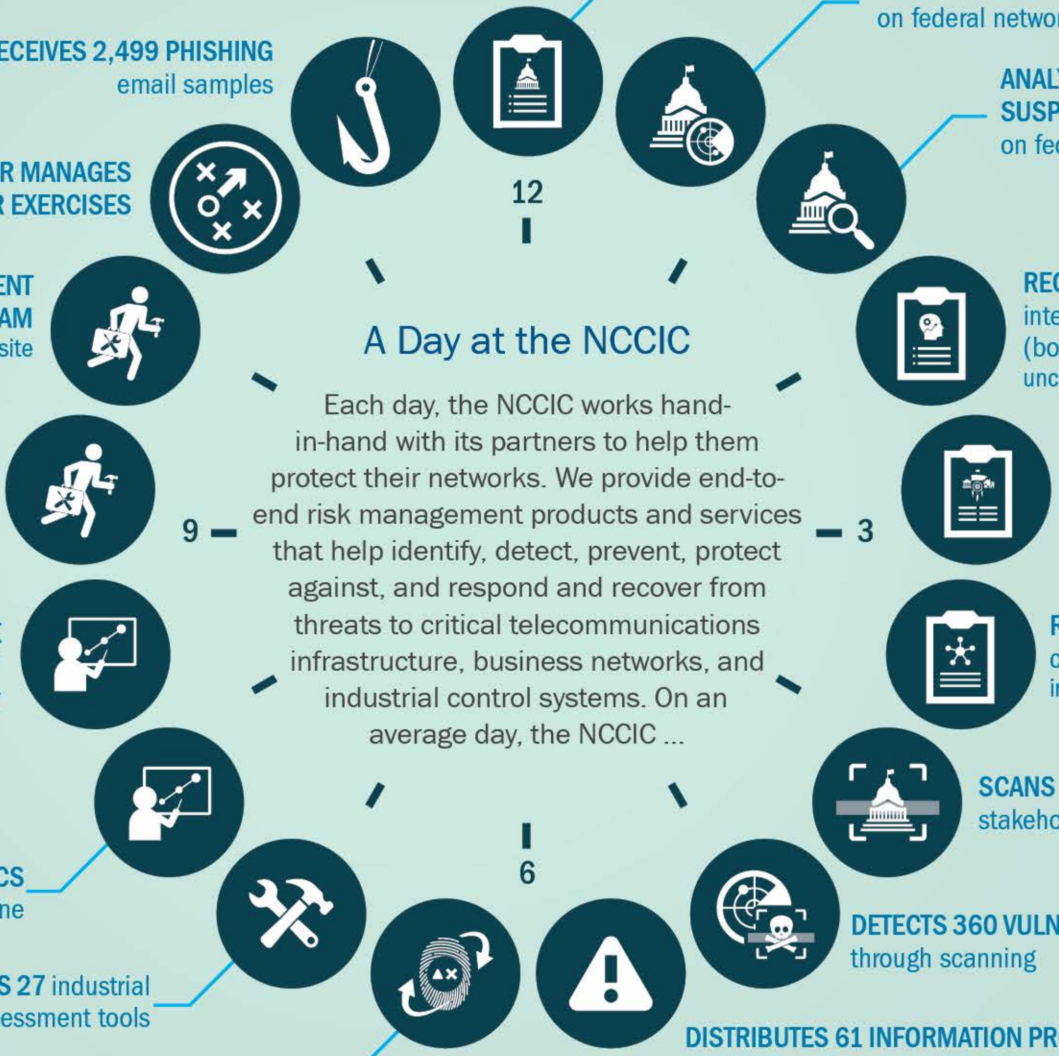
Priorities – CONTINUED

Improve the Nation's readiness posture and understanding of cyber and communications risk through exercises, training, penetration tests, and security assessments.

Defend federal networks through monitoring, intrusion detection and prevention, and incident management.

Expand the community of trusted partners to better share information, exchange technical expertise, and magnify common resources available during times of crisis.

A Day at NCCIC



A Day at the NCCIC

Each day, the NCCIC works hand-in-hand with its partners to help them protect their networks. We provide end-to-end risk management products and services that help identify, detect, prevent, protect against, and respond and recover from threats to critical telecommunications infrastructure, business networks, and industrial control systems. On an average day, the NCCIC ...

Receives **117 INCIDENT REPORTS** from federal departments and agencies

DETECTS THREE CYBER INCIDENTS on federal networks

ANALYZES 207 SUSPICIOUS ALERTS on federal networks

RECEIVES 10 intelligence reporting (both classified and unclassified)

RECEIVES 181 state and local incident reports

RECEIVES ONE critical infrastructure incident report

SCANS 110 stakeholders

DETECTS 360 VULNERABILITIES through scanning

DISTRIBUTES 61 INFORMATION PRODUCTS such as newly identified vulnerabilities and threat alerts

SHARES NINE CLASSIFIED AND 127 UNCLASSIFIED CYBER THREAT INDICATORS with the private sector

DISTRIBUTES 27 industrial control system self-assessment tools

Helps students complete **41 ICS TRAINING MODULES** online

Is **TRAINING 42 PEOPLE** in its state-of-the-art industrial controls system laboratory

HAS THREE NCATS OR ICS-CERT CYBERSECURITY ASSESSMENT TEAMS deployed to partner sites

HAS ONE INCIDENT RESPONSE TEAM deployed to customer site

PLANS OR MANAGES TWO CYBER EXERCISES

RECEIVES 2,499 PHISHING email samples

NCCIC in Action

FY16

BUILDING CYBER AND COMMUNICATIONS SECURITY READINESS

To test its own operational readiness and to support cyber and communications preparedness among all stakeholders, NCCIC conducted a total of **61** exercises in FY16:

- **45** tabletop exercises
- **4** drills
- **9** functional exercises
- **3** full-scale exercises.

NCCIC in Action *FY16*

– CONTINUED

HELPING OUR PARTNERS IDENTIFY AND MITIGATE CYBER RISK

NCCIC conducted **223** "deep dive" risk and vulnerability assessments, including:

- **93** assessments of high-value government and private sector enterprise networks
- **130** assessments of industrial control systems networks

NCCIC ongoing vulnerability scans:

- More than **300** customers assisted
- **12,187** Cyber Hygiene Reports created
- **129,691** vulnerabilities detected

UNCLASSIFIED//FOR OFFICIAL USE ONLY

A - 20170802

NCCIC in Action
FY16

– CONTINUED

RESPONDING TO CYBERSECURITY AND COMMUNICATIONS INCIDENTS

NCCIC received more than **110,361** incident reports from government, critical infrastructure, and international partners in 2016. The NCCIC's incident handlers, analysts, and responders work closely with our customers to triage, prioritize, and provide timely support to help mitigate incidents quickly and to share information to help protect other customers.

NCCIC in Action
FY16

– CONTINUED

BUILDING AWARENESS, EXPERTISE, AND OPERATIONAL PARTNERSHIPS

NCCIC continues to engage the cyber and communications security community to raise security awareness, share best practices and threat and vulnerability information, increase overall technical understanding and expertise, and expand its network of trusted partners.

Information Sharing and Analysis

Automated Indicator Sharing (AIS) is a machine-to-machine capability that receives, processes, and disseminates cyber threat indicators and defensive measures to Federal and non-federal partners.

Cybersecurity Information Sharing and Collaboration Program (CISCP) is a voluntary information-sharing and collaboration program between critical infrastructure partners and the Federal Government.

National Cyber Awareness System (NCAS) offers subscriptions to a variety of cybersecurity information for users with varied technical expertise. NCAS products include Alerts, Bulletins, Tips and Current Activity updates.

National Vulnerability Database (NVD) is the U.S. Government's repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

Information Sharing and Analysis

TLP:RED

Traffic Light Protocol (TLP) provides a set of designations to ensure sensitive information is shared with the correct audience and is based on a trust system with stakeholders.

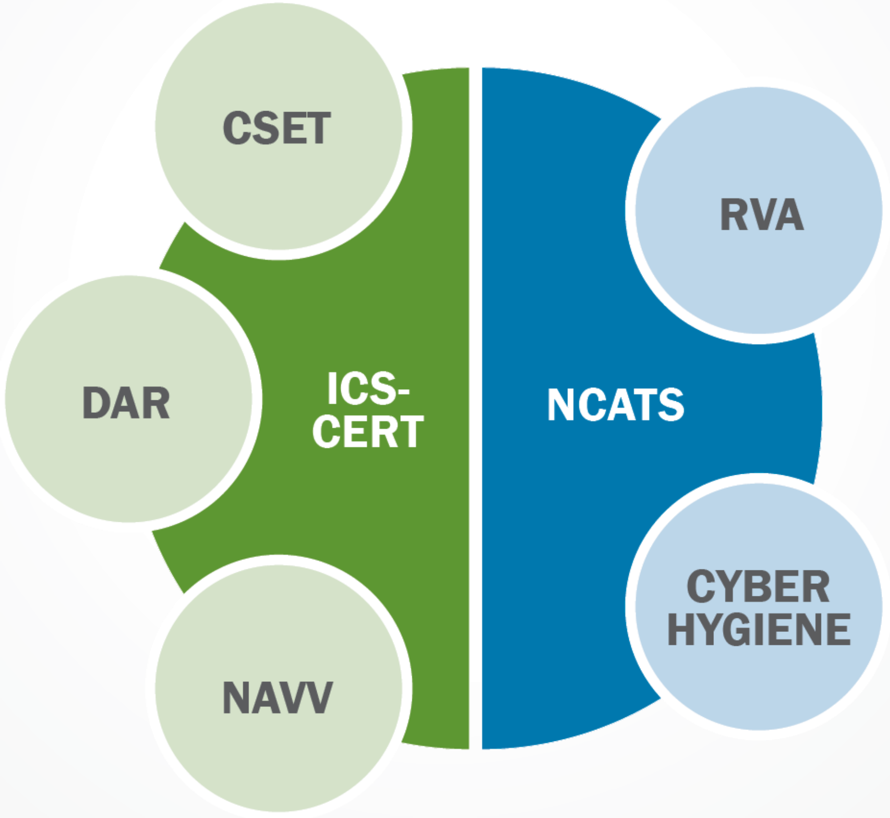
Enhanced Cybersecurity Services (ECS) is a voluntary information-sharing program that assists U.S.-based public and private entities as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration.

The **NCCIC Portal** is a Web-based platform created to give federal agencies, state & local government, and critical infrastructure owners and operators a means to securely communicate, collaborate, and share cybersecurity information.

Cybersecurity Assessments

The **ICS-CERT Assessment Program** provides control-systems focused assessment products, including:

- Cyber Security Evaluation Tool (CSET)
- Design Architecture Review (DAR)
- Network Architecture Verification and Validation (NAVV)



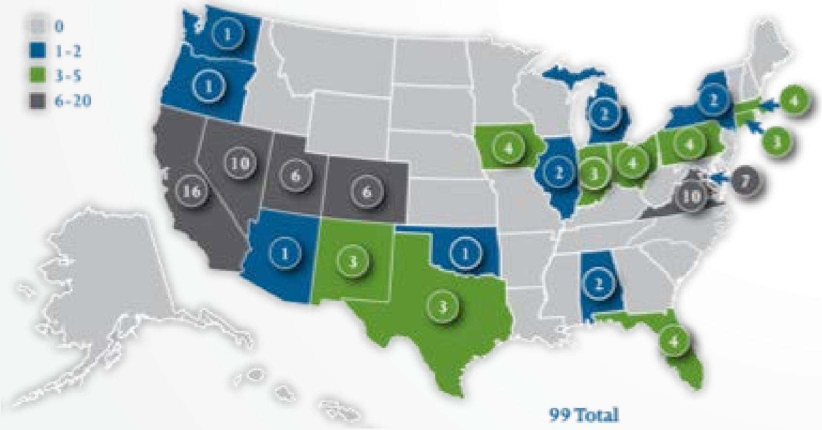
The **National Cybersecurity Assessments and Technical Services (NCATS)** team offers assessment services, including:

- Risk and Vulnerability Assessments (RVA)
- Cyber Hygiene Program

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Cybersecurity Exercises

National Cyber Exercises and Planning Program (NCEPP) develops and supports integrated cyber incident response planning and guidance, and cyber-focused exercises for government and critical infrastructure partners.



National Cyber Exercise Events

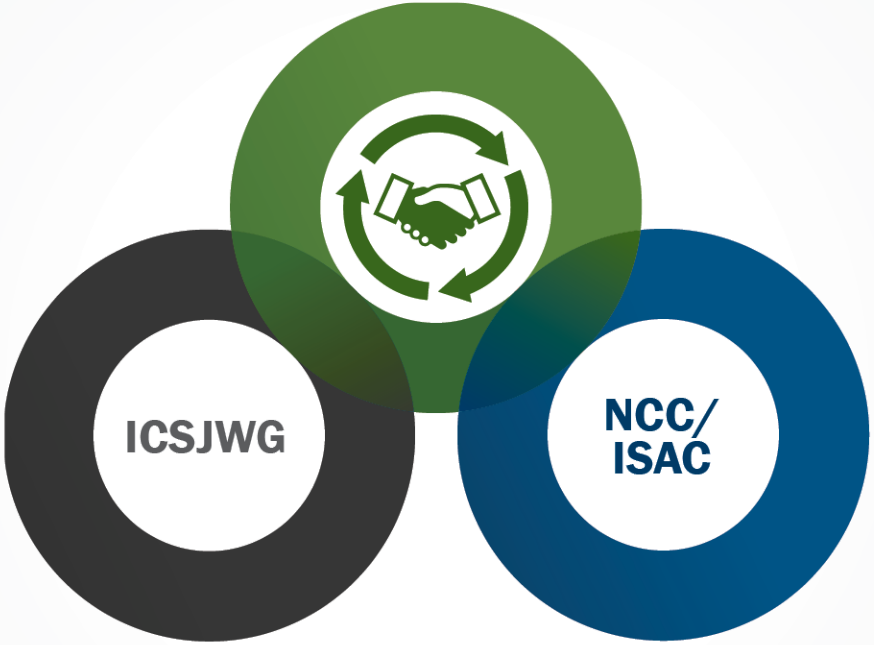
End-to-End Cyber Exercise Planning and Conduct

Cyber Exercise Consulting and SME Support

Cyber Planning

Off-the-Shelf Resources

Public-Private Partnerships



The **Industrial Controls Systems Joint Working Group (ICSJWG)** provides a forum for communication among ICS stakeholders, to include critical infrastructure and federal entities, as well as private-sector owners and operators.

The **National Coordinating Center (NCC)** is designated as the **Information Sharing and Analysis Center (ISAC)** for communications. The ISAC facilitates exchange of vulnerability, threat, and intrusion information among government and industry.

Federal Network Protection

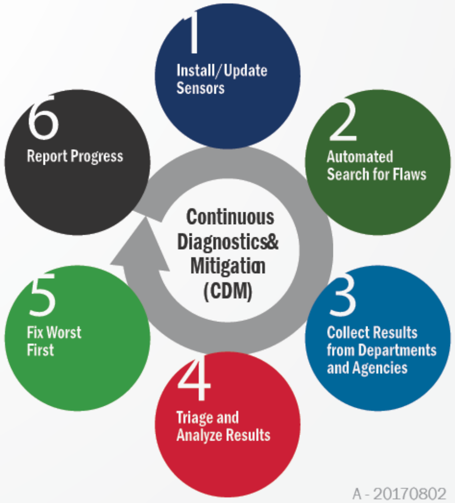
EINSTEIN provides the Federal Government with early warning detection including:

- Near real-time identification of malicious cyber activity
- Prevention of malicious cyber activity

PROTECT
DETECT
ANALYZE

The **Continuous Diagnostics and Mitigation (CDM) Program**:

- Provides NCCIC with an enterprise-level dashboard to view the risk posture of the participating federal agencies


Continuous Diagnostics& Mitigation (CDM)
1 Install/Update Sensors
2 Automated Search for Flaws
3 Collect Results from Departments and Agencies
4 Triage and Analyze Results
5 Fix Worst First
6 Report Progress

A - 20170802

Watch Floor Operations

24/7

DAILY

NCCIC maintains 24x7 watch operations across three physical locations: Arlington, VA; Pensacola, FL; and Idaho Falls, ID. Each watch floor centralizes NCCIC's incident response and information sharing activities.

Every day, watch floor incident handlers triage and disperse hundreds of incidents and suspicious activity reports to NCCIC analysts for resolution.

NCCIC co-locates partners from the intelligence community, federal departments and agencies, state and local governments, and the private sector.

Incident Response and Recovery

Incident Response Teams (IRT) provide intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance.

- IRT performs on-site and remote response services.
- Engagements include log, network traffic, and host analysis.
- Rapid response teams (deployed within 8 hours) are available.

NCC leads efforts to ensure resilient National Security and Emergency Preparedness (NS/EP).

- Advises the President on NS/EP communications decisions during a national emergency.

NCC supports Emergency Support Function #2

- Communications under the National Response Framework

UNCLASSIFIED//FOR OFFICIAL USE ONLY

A - 20170802

Incident Response

Case Study: OPM

JUNE 2015:
OPM announced that it had once again been the target of a massive data breach potentially affecting millions of Americans.

Initial breach discovered in early 2014 and compromised information about OPM servers, but no PII

This recent breach compromised the PII of approximately 21.5M people, according to the agency

- 19.7M personnel that applied for security clearances
- 1.8M family members

OPM discovered the most recent intrusion on its own using tools that were recommended by US-CERT following the initial intrusion

Incident Response

CONTINUED

Case Study: OPM

Based on guidance provided by US-CERT during mitigation of an earlier cybersecurity incident, the organization began implementing improved cybersecurity capabilities across its networks.

US-CERT substantiated the compromise using EINSTEIN and assessed the potential damage. SMEs from the interagency response team provided guidance in numerous specialized areas such as IBM mainframe and web applications.

US-CERT was provided with digital media for analysis. Analysis of these artifacts led to the identification of the tools used for remote access and lateral movement by the advanced persistent threat (APT) actor.

US-CERT developed indicators of compromise (IOCs) that were shared with trusted partners. IOCs were also used to develop signatures for EINSTEIN.

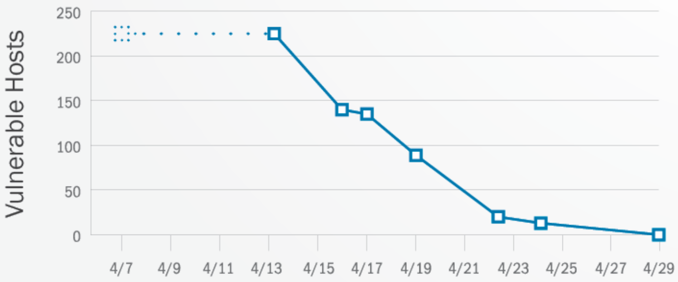
Cyber Hygiene

Case Study: Heartbleed

APRIL 2014:

Reporting of Heartbleed (CVE-2014-0160) is made public by OpenSSL. This weakness allows stealing the information protected by the SSL/TLS encryption used to secure the Internet. Examples of the affected applications are web, email, instant messaging, and virtual private networks.

VULNERABLE HOSTS FOUND OVER TIME



System software and hardware infrastructures affected by this vulnerability include: Amazon, Cisco, Linux, F5, Fortinet, Google, HP, IBM, Intel, Juniper, McAfee, Oracle, Symantec, and VMware.

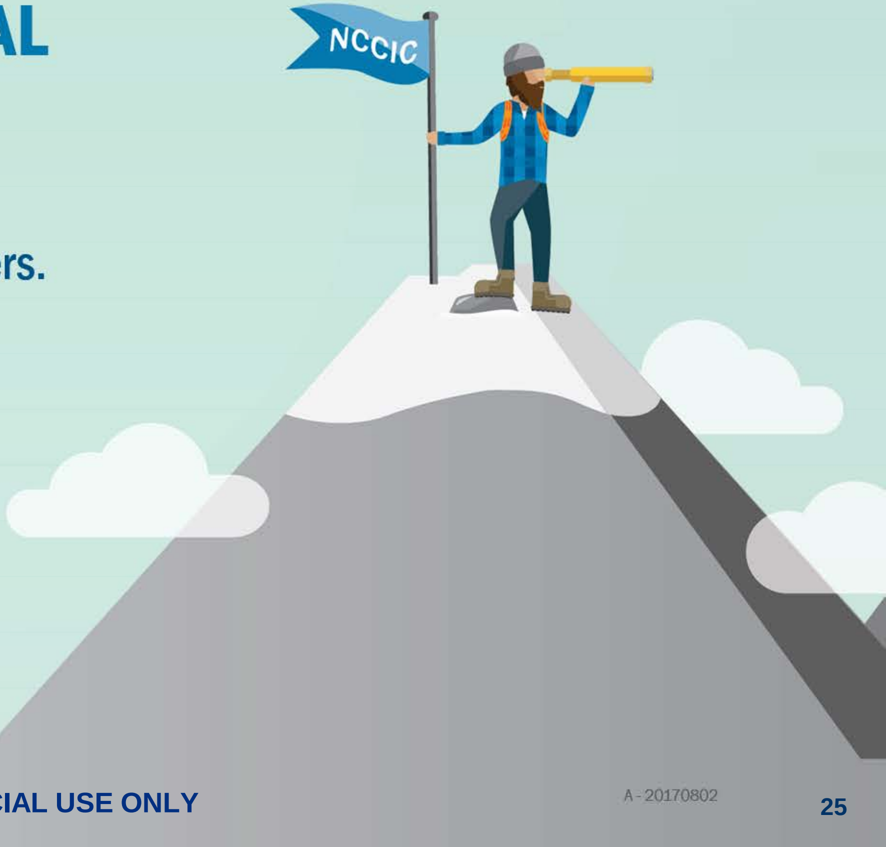
NCCIC worked with more than 100 federal agencies, received authorization, identified public IP address space, scheduled times to conduct scanning, and delivered individualized reports and results to each agency.

NCATS scanned federal IP space of an estimated 15.5 million IPs and assisted in reducing the number of federal Heartbleed occurrences. This was a 99 percent reduction in Heartbleed instances across the federal government within a three week period of time.

Conclusion

AS NCCIC CONTINUES TO BUILD, EXPAND, AND IMPROVE THE PRODUCTS AND SERVICES IT PROVIDES, THE RISK TO NATIONAL INFRASTRUCTURE EVOLVES.

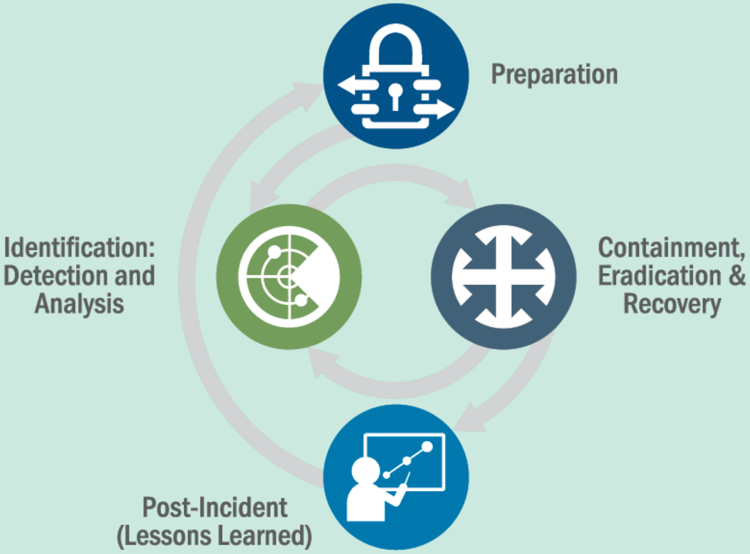
Staying ahead of the threat curve requires sustained participation of public and private sector stakeholders. Together, we must anticipate, adapt to, and defend against emerging threats.



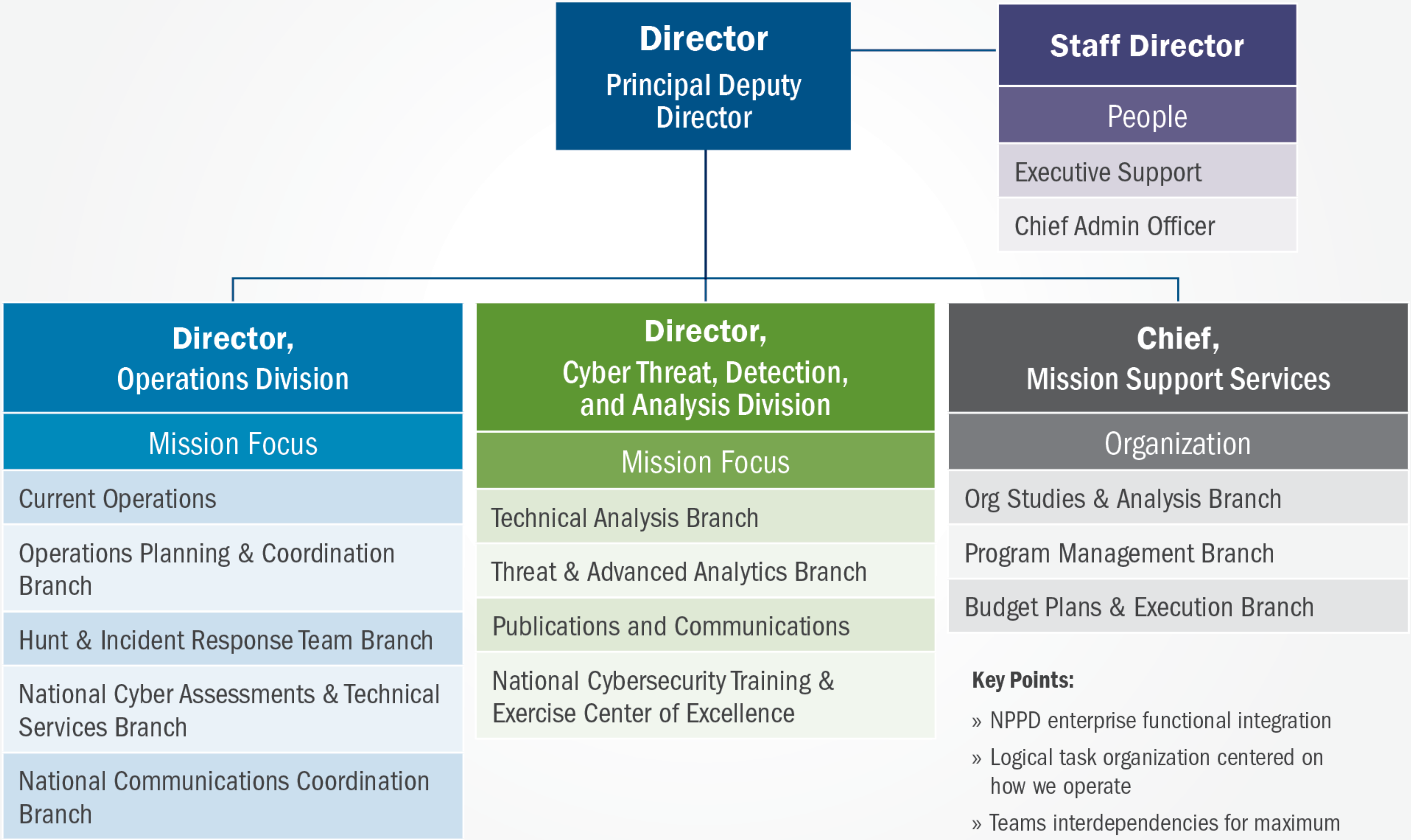
Conclusion

Over the next year, NCCIC will aggressively pursue the following practical priorities:

- Listen to our partners and constituents to ensure that DHS remains responsive to their needs and closes gaps in services.
- Expand the network of AIS users, and encourage active participation in all information sharing programs, in order to improve the nation’s security posture.
- Ensure NCCIC practitioners receive the tools and training necessary to remain leaders in the field, and continue to recruit technical experts to support mission success.
- Optimize resource utilization and achieve demanding program performance metrics by refining processes, technology, and organizational structure.


Preparation
Identification: Detection and Analysis
Containment, Eradication & Recovery
Post-Incident (Lessons Learned)

NCCIC Organization Structure



Director
Principal Deputy Director

Staff Director
- People
- Executive Support
- Chief Admin Officer

Director,
Operations Division

Mission Focus
- Current Operations
- Operations Planning & Coordination Branch
- Hunt & Incident Response Team Branch
- National Cyber Assessments & Technical Services Branch
- National Communications Coordination Branch

Director,
Cyber Threat, Detection, and Analysis Division

Mission Focus
- Technical Analysis Branch
- Threat & Advanced Analytics Branch
- Publications and Communications
- National Cybersecurity Training & Exercise Center of Excellence

Chief,
Mission Support Services

Organization
- Org Studies & Analysis Branch
- Program Management Branch
- Budget Plans & Execution Branch

Key Points:

» NPPD enterprise functional integration

» Logical task organization centered on how we operate

» Teams interdependencies for maximum effectiveness

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Questions

CONTACT NCCIC:

NCCICCustomerService@hq.dhs.gov

888-282-0870

+1 703-235-5110

U.S. DEPARTMENT OF HOMELAND SECURITY

NCCIC